PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/40 — A1

(11) International Publication Number: WO 97/13208

(43) International Publication Date: 10 April 1997 (10.04.97)

(21) International Application Number: PCT/US95/12459

(22) International Filing Date: 6 October 1995 (06.10.95)

(71) Applicant *(for all designated States except US)*: SCIENTIFIC-ATLANTA, INC. [US/US]; One Technology Parkway, South, Norcross, GA 30092 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: HOUSER, Peter, B. [US/US]; 14574 High Pine Street, Poway, CA 92064 (US).

(74) Agents: POTENZA, Joseph, M. et al.; Banner & Allegretti, Ltd., Suite 1100, 1001 G Street, N.W., Washington, DC 20001 (US).

(81) Designated States: CA, JP, MX, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

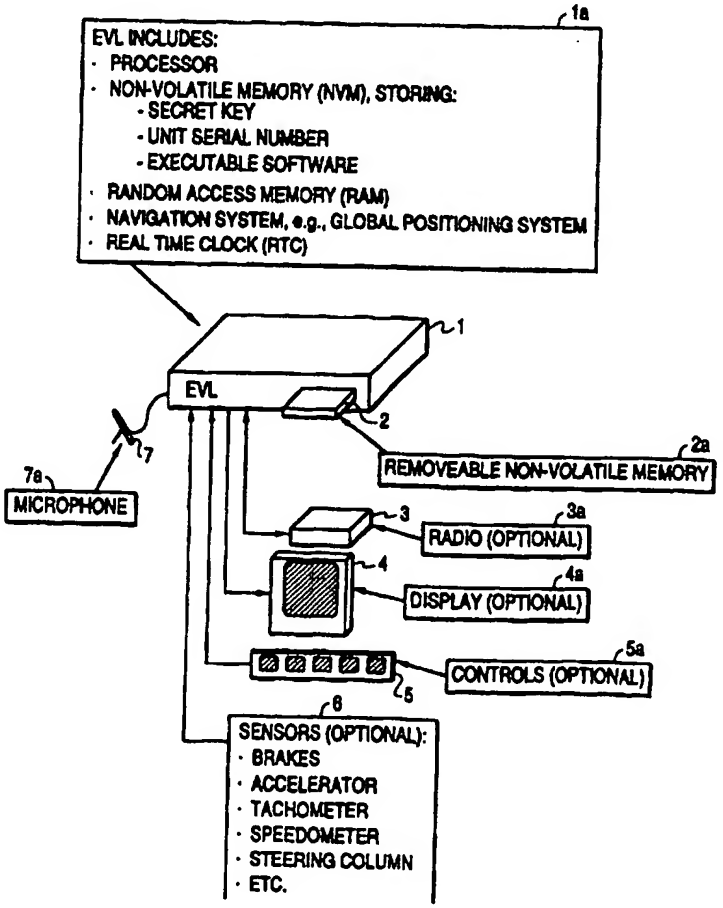
Published

With international search report.

(54) Title: ELECTRONIC VEHICLE LOG

(57) Abstract

A method and apparatus for maintaining an electronic vehicle log (1) involves the formation of protected data packets (411) which are electronically signed by certified users. The electronic vehicle log (1) preferably comprises a secure non-volatile memory (2) that may be removed from the vehicle (200). Preferably the apparatus, referred to herein as a date processing interface unit (DPIU) (1), has access to date and real time of day and location data so that the protected data packets (411) further include, besides data to be protected, the date and time of day and the location of the vehicle (200) for comparison with expected data as further protection against fraudulent or forged data entry. Preferably, on-board sensors (6) collect in-transit monitoring and cargo monitoring data for access by various certified users. Event data such as governmental inspection or border crossing data may be entered into the log by governmental authorities.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

ELECTRONIC VEHICLE LOG

BACKGROUND OF THE INVENTION

1. Technical Field

This invention relates to the field of electronic vehicle logs used particularly in commercial vehicles and, more particularly, to a data collection and processing system for a vehicle serving multiple users including the driver, the owner/operator and governmental authorities. Even more particularly, the invention is directed to securing access to particular data by such users via the application of evolving "smart" or "flash" card, public key/private key encryption and electronic signature, speech recognition and speaker verification and global positioning or other navigation system technologies.

2. Description of the Related Arts

Many vehicles, particularly those used commercially, must maintain legally auditable records of their usage. These records may include and not be limited to include data items such as license or registrations issued, insurance coverage, the routes traveled, gross and tare (cargo exclusive of container and vehicle) weight measured at weigh stations, driver and duration of driving, safety inspection results, border crossing approval, exhaust pollution measurements and the like. In addition to vehicle related items, additional data may be required concerning the cargo and any tariffs or other fees paid on that cargo. Other records may also be required or used by the driver, the owner/operator (if different), and governmental authorities or agencies.

For the purposes of the present application, vehicle credential data is defined as data describing the vehicle, the carrier, cargo, driver, and passengers independently of the transit involved. Vehicle credential data may thus include the following data, the following list being exemplary of such data: vehicle registration, vehicle insurance, driver's license, driver's credentials, driver's safety record and health, cargo manifest and shipping invoice, tariff-related documentation, and declared itinerary or intended route data.

In-transit data is defined for the purposes of the present application as data obtained during transit or in route (whether the vehicle is in motion or not). Such data may be acquired by periodically monitoring sensors on the vehicle to determine how the vehicle is being used. Exemplary data falling into this category of data

include: date and time of data collection, vehicle speed, brake usage, steering wheel motion, engine RPM, engine temperature, cargo container temperature, engine vibration and other health metrics, and vehicle location from a navigation source such as the so-called Global Positioning System (GPS) or equivalent data gathering system.

Cargo monitoring data is defined for the purposes of this application as data related to either the status or security of the cargo, for example, whether the cargo seal has been maintained or broken.

Next, event record data is defined for the purposes of this application as data recorded in transit for particular events effecting the vehicle or cargo or both. Typical events include: vehicle weight, for example, obtained during a weight-in-motion or stationary scale weighing, vehicle environmental, emissions or safety status checks, for example, determined at an inspection facility, border crossing data, either state or national, hazardous material (HAZMAT) warnings or transit regime changes (when the vehicle starts motion or has stopped).

Finally, route monitoring data is defined for the purposes of the present application as data obtained through monitoring the vehicle in transit to compare with the above-defined vehicle credential data for an intended route. This data is preferably collected through the application of a navigation system such as GPS or other equivalent system as well.

Typically in the past, such records, if maintained at all, have been manually maintained in a handwritten log or plurality of such logs, augmented by inspection records from various agencies or authorities and maintained by the driver. However, such handwritten logs are inherently subject to inadvertent inaccuracies, as well as to intentional fraud or forgery. In addition, such handwritten records cannot be easily transferred for inspection.

Ebaugh et al., US Patent No. 5,303,163, describes a configurable vehicle monitoring system having first and second configuration levels for an owner/operator and a driver respectively. Besides being able to independently configure data in memory, each is independently able to access certain data of interest to that party alone. The data that can be gathered and analyzed includes miles per gallon, fuel consumed, trip time, idle time, fuel consumed and other pertinent information relevant to fleet or vehicle operation. For example, according to Figure 7 thereof,

a printout may be obtained showing these and other data. The owner/operator may obtain an indication of the period of time the vehicle is operated in excess of the 65 mile per hour overspeed limit. Similarly, apparatus disclosed by Ishibashi, US Patent No. 5,379,219, and Komatsu, US Patent No. 5,249,127 suggest the tracking of speed over time and, per Figure 3 of the '219 patent, the allocation of memory among ID data, speed data, travel distance data and optional area. The '127 patent suggests that, memory size requirements being indeterminate and expensive, data compression devices be provided for assuring efficient utilization of memory.

It has further been recognized that portability of the collected data is required. One means of achieving portability is via an external memory module (US 4,757,454, 5,185,700 or 5,249,127). Also, radio or generally wireless radio communication may provide data mobility from one user to another (US 4,804,937, 5,185,700 or WO 90/09645).

The so-called global positioning system described, for example, by Taylor et al., US Patent No. 4,445,118 and O'Neil et al. US Patent No. 4,839,656 has been implemented in an electronic vehicle log by Haendel et al., US Patent No. 5,359,528. Haendel et al. describe that a change in state boundary and a log of miles within a particular state may be automatically obtained without driver intervention.

All of these systems suffer from a lack of security of access by a particular user and may be falsified if and when the provided weak security systems fail. It is an object therefore of the present invention to describe a system whereby multiple users of a system may configure or obtain access to memory of an electronic vehicle log. It is a further object of the present invention to provide a system wherein security is enhanced via adaptation of evolving technologies of speech recognition and speaker verification, public/private key data encryption and decryption, flash or smart card (key) access and/or electronic signature record verification and access.

SUMMARY OF THE PRESENT INVENTION

In accordance with the present invention, an electronic vehicle log (EVL) comprises a processor for processing data, a memory for storing software algorithms and fixed data, preferably non-volatile in nature, a secret key unique to the vehicle log, and a unit serial number that is unique to that unit (hereinafter, an EVL identifier), a removable non-volatile log memory for securely recording data and a

navigation and time-of-day and date input data circuit. In one embodiment, there may be further provided a microphone input for receiving user speech coupled to the processor (for example, via an analog to digital converter) and a memory for storing digitized voice samples. Optional sensors are coupled to the log for providing for the input of data for vehicle and cargo, for example, through an external interface, in particular, a wireless interface. For example, through one external wireless interface, an EVL may acquire event data such as weight-in-motion (WIM) data. Those who would obtain access to data or input data are provided with a public key which is likewise unique to the vehicle log. Moreover, any data entries are signed with an electronic signature for verifying the entered data, for example, comprising a calculated hash value encrypted with the secret key.

When the vehicle is to be used, the driver inserts the removable non-volatile log memory for the duration of the trip. For example, a driver may obtain access and log into the EVL by inputing their speech, a password or a biometric after inserting their card memory. Upon successful verification of the password or biometric and, if appropriate, verification of the speaker's identity in a well known manner, the driver-unique data is used to decrypt a secret key member of a public key encryption pair. When data is to be logged by the driver, protected data packets (PDP's) containing this log data are generated with digital signatures formed by encrypting digital hash values with this secret key member of the public key pair.

Protected data packets (PDP's) are transmitted to a requesting user via electronic means, for example, wireless, telephone modem or a memory card. The requesting user has a trusted (escrowed) copy of the public key of the above-referenced public key pair, the public key pair including the secret key (securely stored in and never released from EVL memory) used for forming the electronic signature. The secret key should be protected and secured as closely as possible and should not be transmitted (otherwise, it might be intercepted by an uncertified individual). The public key is used to verify that the electronic signature of the PDP is accurate. Correct verification of the electronic signature then confirms the data source (the driver-protected secret key) and the integrity of the data (since the hash value matches the PDP data).

A governmental authority may obtain access by a defined process. One

example of such a process for obtaining an early transmission of vehicle data in advance of a border crossing or like event is described by the following. The agency wishing to receive secure data generates a public key encryption pair different from that used by the driver and distributes the public key portion to any person or system desiring to transmit secure data. The public key portion is stored in EVL memory. A profile of a commercial vehicle and a cargo may be extracted from the vehicle via a card memory or may be electronically extracted by wireless means prior to the vehicle's departure and delivered to the authority with the stored public key portion. The EVL generates a private encryption key and uses it to encrypt PDP's with their corresponding digital signatures. The EVL encrypts this private encryption key using the public key and transmits that information to the agency receiving the data. The receiving agency decrypts the EVL private encryption key using the secret key portion of the key pair and then decrypts the PDP's using the decrypted key. The profile and public key are transmitted via a centralized authority data base to regional data bases for distribution to checkpoints, port of entry border crossings and the like along the intended route of the vehicle.

As the vehicle approaches the inspection facility, the vehicle is polled or interrogated, for example, preferably by wireless means in advance of reaching the facility, so the vehicle need not stop its movement. The vehicle transmitted profile data is compared with the previously transmitted profile data and the inspector may preclear the vehicle through the inspection station. If the inspection data is a weigh station, for example, and data is to be entered into the log by the authority, an electronic signature is utilized to verify the entered data, preventing subsequent modifications of the logged information. Moreover, at the time the entry is made, the vehicle position and time from the global positioning system may be automatically and simultaneously recorded, allowing detection of fraudulent entries. As the vehicle crosses the border, a short range communications system may be used to verify that the vehicle crossing the border is the vehicle which received the preclearnace to cross.

It is also possible that the vehicle may carry all the profile information in the EVL and transmit the data via wireless means to the authority just a few minutes before the approval (for example, preapproval at a border crossing) event. In this

case and in that described above as well, some sort of short-range transmission is useful as the vehicle crosses the border to physically confirm that the vehicle currently crossing the border is the same as the one that provided the profile and credentials and received preapproval to cross.

An authorized individual such as an inspector or police officer creates a digital credential in a generating device's memory, for example, a laptop personal computer. A secret key of a public key pair is used to generate a digital signature for the credential data. The credential and signature are transmitted to the EVL using various means, possibly including wireless means, direct input (typing), or memory card transfer. This transfer may be encrypted as discussed above as desired. for wireless or other secure data transmission. The credential and signature are formed into a PDP and logged as described above for the driver data logging operation. When the credential is subsequently transmitted to a requesting agency, the agency will use a trusted copy of the public key portion to verify the electronic signature of the PDP.

Other features and advantages of the present invention will be explained by reference to the drawings and the following detailed description of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an overview drawing of an electronic vehicle log according to the present invention;

Figure 2A is a system overview drawing showing the interface between a vehicle 200 carrying an electronic vehicle log of Figure 1 with a governmental or other authority and Figure 2B shows vehicle 200 with expanded boxes describing data that may be stored in DPIU 210 including an electronic vehicle log of the present invention;

Figure 3 is a schematic block diagram of the electronic vehicle log of Figure 1 for maintenance in a vehicle; Figure 3A provides a first embodiment, Figure 3B provides a second embodiment and Figure 3C provides a third embodiment;

Figure 4A provides an overview of the key and security features of the present invention in flow diagram form and Figure 4B shows a table showing the use of different public key pairs by different entities for accessing the data stored in the EVL

400 of Figure 4A;

Figure 5A provides a table of examples of data maintained in an in-vehicle data base of memory of the in-vehicle unit of Figure 4; Figure 5B comprises a table showing data elements and characteristics recoverable through utilization of the present invention and their characteristics; and

Figures 6A and 6B provide a table showing service, application, technology or product availability, demonstrable feature and utilization of the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

Referring to Figure 1, there is shown an overview drawing of the electronic vehicle log of the present invention. The present device is intended to be placed in a vehicle, hence, the present invention is described herein as an in-vehicle data processing unit. The log is described herein as electronic because it generally operates via electronic circuits including at least memory circuits and a data processor. The present invention is characterized as a log because the memory of the present invention substitutes for prior art hand-written log books typically used by drivers of vehicles, especially commercial vehicles.

The electronic vehicle log (EVL) 1 is described by box 1a as comprising a package of elements suitably housed to be mounted in a vehicle, for example, in an operator compartment or secure area therein or proximate thereto. One mounting arrangement would be to provide a bracket mounting plate permanently secured to the vehicle. The EVL housing, herein referred to as a data processing interface unit (DPIU) then is removably secured thereto by mechanical locking apparatus so that the DPIU may be removed from the vehicle as necessary. The mechanical locking apparatus should be tamper-resistant so that the EVL itself cannot be surreptitiously moved from one vehicle to another without detection. (To accomplish this objective, electronic tamper detection may be employed). Preferably, the DPIU housing is adapted to receive a removable security module as will be further described herein which is the electronic vehicle log itself.

The EVL housing 1 (DPIU) contains a processor, preferably a microprocessor and a non-volatile memory coupled thereto for storing at least secret key data, secret EVL unit serial number data and executable software. The EVL 1 further may comprise a random access memory that typically is volatile for storing data on a

temporary basis and a real time clock (typically a software algorithm that is preferably periodically updated). Most processors require a clock oscillator output that is controlled for providing processor operation clocking functions. This clock can provide a clocking input to a real time clock algorithm as is well known in the art. However, for greater security, an independent clock source may be used or an internal isolated hardware clock circuit (not shown). A navigation system such as the Global Positioning System (GPS) or Loran or other system can provide the independent clock source or periodic indications as to true time for synchronizing a local real time clock as is likewise known in the art. Of course, another important function of GPS or other known equivalent systems is the provision of periodic location data in the form of earth latitude and longitude data and even altitude data that may be compared with a map or intended route and thus provide specific data as to real time of day and route location. A further description of preferred embodiments of EVL 1 will be provided in connection with applicant's description of Figure 3.

EVL housing 1 has insertable therein a removable non-volatile memory module 2 described by box 2a which becomes the log in place of known paper logs or other known electronic logs. In accordance with the present invention, the log memory 2 stores secured or protected data packets output from the EVL included processor as will be further described in connection with Figure 4.

The EVL 1, according to the present invention, may communicate with governmental authorities via radio 3, according to box 3a which may be optional or through wired or other means. Certainly by radio is intended communication via all radio frequencies including light frequencies or via laser or other known means that is wireless in nature. As will be further described herein in the example depicted in Figure 2 of a border crossing, the EVL communicates with an inspection facility for border preclearance before reaching the border via wireless means, so the vehicle need not stop.

The EVL 1 may be provided with a display or other output means 4. The display, as indicated by descriptive box 4a, may be optional. The display may comprise a liquid crystal display, cathode ray tube display, light emitting diode or other display. Other output means may comprise a printer or speech synthesis means

or other output means. All such means provide the user (typically the vehicle operator) with feedback of proper operation, an indication that the vehicle is being polled, clearance to proceed, log data, if appropriate, and other information.

Controls 5, as described by box 5a, are likewise optional. The controls typically comprise a keyboard, keypad or related switch control but may comprise speech receiving means 7 described by box 7a as a microphone such as an electret microphone or digital microphone. Also, both keys and microphones may be provided. The microphone may be eliminated if speech input is not contemplated by one designing a system according to the present invention. The controls may be keys representing, for example, numeric or alphabetic characters for inputing the operator's identity, password or other data as will be described further herein. If necessary the microphone is coupled to the processor of the present invention via an analog to digital converter for sampling the voice input and converting the input to digital samples.

Finally, in accordance with Figure 1, sensors 6 may be provided which are only generally described. These may comprise brake sensors, accelerator sensors, tachometer or mileage sensors, speedometer sensors, steering column sensors, tire pressure monitoring sensors, cargo bonding sensors, cargo temperature or smoke or fire sensors, driver alcohol (breath) detection sensors and the like which may be coupled to EVL 1 by wired or wireless means.

In-transit, cargo and route monitoring data use sensors which are preferably mounted on the vehicle and locally communicate with the EVL using fixed communications channels (cabling or short-range radio signals). Credentials and event data recording typically requires acquiring data from systems separate from the EVL housing 1 which are not permanently mounted on the vehicle. For example, a customs agent may be empowered to record a credential within the EVL which indicates that paperwork is in place and tariffs paid to allow expedited international or state border crossings as will be described further in reference to the example of Figure 2. This credential information is placed within the EVL by any number of transmission methods and via security means including direct entry, via a removable credential memory, via direct connection and via radio connection.

In regard to direct entry, the EVL 1 may provide a keyboard and limited

display for manual entry of the information. This may be relatively tedious and insecure. The entry process may include the agent (inspector) specifying an encryption key, either public or private, which may be used in a signature process for authenticating entered data. The process may involve speech recognition and voice entry of the data in combination with a keyboard/display or alone. The process may further comprise speaker identification or verification processes known in the art for confirming a subject's claimed identity based upon a digitized speech sample.

Removable credentials are preferred. If the EVL memory is removable, it may be placed in a data entry device belonging to the agent and the electronic credential or event data copied into the memory. When the memory device is replaced into the EVL 1, the newly acquired data will be processed as a normal PDP as described below in connection with Figure 4.

Direct connection may be cumbersome. The EVL may be directly cabled to the agent's data entry device, using a media such as an RS 232 serial data channel or equivalent serial or parallel connector. Data processing in this case is comparable to that when using removable credentials.

Finally radio connection may be preferable for, for example, coupling to mobile police forces, air such as helicopter carrying radio, or roadside radio polling stations so the vehicle may transmit in motion. Radio may be used to receive or transmit credential and event data. One example is a weight in motion (WIM) station operated by a governmental authority. A WIM sensor may, when interrogated by the EVL, transmit the vehicle's weight to the EVL for storage.

As will be further described in connection with Figure 2, an agent uses a personal computer or workstation to generate, for example, border crossing or inspection credential data. An agent-specific secret key is used to embed their electronic signature within the credential data transferred to the EVL 1. Thus, the data may not be accessible to the driver or even the vehicle system operator. When the credential data is later transmitted to an authorizing agent (such as the border crossing inspector), the corresponding public key is used to decrypt the signature, thereby authenticating the source and permitting preclearance of the vehicle.

Now, referring to Figure 2, one application of the present invention will be described, namely a border crossing, to demonstrate the interrelationships among the

elements of Figure 1 which may be assembled in combination to perform any desired application of the present invention. Figure 2 generally represents in diagrammatic form the events at a border crossing of a vehicle 200 equipped with the EVL 1 (Figure 1) of the present invention (represented as box 210). Other applications will be described subsequently herein. Vehicle 200 may be a truck, for example, approaching a border crossing 202 which may be a state or international border along a route 201. There are three zones of route 201 the vehicle 200 is expected to pass through. Zone 205 comprises a reporting zone. Zone 206 comprises an evaluation/clearance zone. Zone 207 comprises an inspection zone for performing a detailed inspection, as necessary, of vehicle 200 or health check of the vehicle's driver. The arrows on route 201 indicate the expected direction of passage of vehicle 200.

Referring briefly to Figure 2B, there is shown a typical vehicle 200 and blocks 261-266 summarizing data that may be related thereto. Block 261 describes motor vehicle data such as ID number, EVL or DPIU identification number and status, vehicle weight and registration data. Driver data 262 comprises their identification, their licenses, safety record, transit log and safety biometrics among other data. Carrier data 263 includes identification, location, registration, insurance, licenses and permits, ICC, PUC, USDOT records, violations and offenses and fees paid records. Cargo data 266 includes trailer identification, invoice, manifest, HAZMAT warnings, gross and tare weight, export declaration, inspection record, tariff record and crossing approval data. Together, these data 261, 262, 263 and 266 may be vehicle credential data as used in the context of the present application.

Transit security block 264 refers to electronic bonding data, route verification data and time-in-travel verification data.

Safety and environmental data block 265 refers to a combination of event data and in transit data. In particular, block 265 refers to inspection records, emission records on-board sensor records and HAZMAT warnings.

Typically at a border 202 or proximate thereto is an inspection facility 203. At the inspection facility, work stations, shown as computer workstations, 204 are provided governmental employees, such as inspectors. The work stations and/or inspection facility 203 preferably communicate with vehicle 200 which may be

moving by wireless means. The PC-based inspector workstations 204 are described by box 220. The workstations function to interface with an interface unit described by block 210 usually referred to herein as the EVL of vehicle 200 and to roadside sensors of a polling station (not shown). These sensors respond as a vehicle passes a polling station in motion to obtain data from the EVL. These may not need be "roadside" but may be "fly over" and thus mounted in aircraft such as helicopters or other traveling vehicles such as police vehicles. In any event, the workstations 220 function to record electronic credentials either downloaded in advance or provided from the EVL 210 of the vehicle 200. The workstation 204 may interface with centralized databases to obtain data that is not stored in the workstation as necessary. Finally, it is desirable if the workstations 204 are networked together for intercommunication and interchangeability. That is, if one workstation is occupied, a first spare workstation is allocated to an new incoming vehicle 200 to the system.

The work stations 204 and/or inspection facility 203 generally are provided with an EVL interface unit for interfacing with the in-vehicle EVL 1 of vehicle 200. The functions of this interface unit are described by box 210 which couples the inspection facility 203 or workstation 204 or both with the EVL resident in vehicle 200. This interface unit carries and provides credentials/manifests/inspection records collected for a vehicle. The interface unit also collects multi-sensor reports from on-board sensors on the commercial vehicles such as vehicle 200, for example, on odometer readings, brakes, cargo bondings and the like as optionally provided. Moreover, the interface unit provides vehicle to roadside (or fly over) polling stations communication between the EVL and the governmental employees such as inspectors and inspection stations such as weight-in-motion measuring stations. The latter data may be recorded in the EVL as will be described in connection with Figure 4 as protected data packets. Another function of the interface unit is general information management and the updating of the EVL data base and records due to governmental activity. For example, the opportunity for preclearance of a vehicle through an inspection station is one type of data that may be entered into the EVL. Finally, the interface unit provides electronic security in accordance with the security features described by Figure 4. Communications to and from the vehicle 200, especially if wireless, are preferably secured from interception by coding and/or encryption as

desired.

In operation, a vehicle 200 moves along route 201 into a reporting zone 205. The vehicle 200 may initiate radio contact with inspection facility 203 or the vehicle may be polled via roadside or other monitors. Meanwhile, manifests for the vehicle and associated data are preferably electronically downloaded by a broker (a carrier or other party) for storage at the facility 203. Current manifests of expected vehicles are provided to individual inspector workstations 204. Responsive to a polling signal or associated with a request for preclearance initiated by the vehicle, the vehicle data of particular vehicle 200 is provided via wireless means to inspection facility 203 and compared at workstations 204 with downloaded data, such as manifest data. On-board the vehicle, the driver may be provided with a display indicating the EVL is being monitored and thereby reported to him. Moreover, a report or record of the monitoring activity may be stored in the EVL along with a real time of day and location indication as will be subsequently described herein.

The vehicle then enters an evaluation/clearance zone 206. The governmental authority such as an inspector assesses the records/data obtained from the EVL at his workstation 204. If the inspector is satisfied, the inspector communicates a bypass or, if not satisfied, a no-go signal to the truck. Of course, the EVL records and updates itself according to the bypass or no-go signal. As the vehicle approaches the border 202, roadside monitors may poll the vehicle in transit as it crosses the border to assure that the vehicle crossing the border is in fact the vehicle given preclearance to cross. There exists the possibility that preclearance may not have been received in a timely manner even though preclearance could have been granted as the vehicle enters the inspection area 207. Vehicles not receiving timely preclearance and vehicles whose credentials are suspect may be signaled to stop in inspection zone 207.

As the vehicle 200 moves it will enter a detailed inspection area indicated as such on route 201. Inspection zone 207 corresponds thereto and, at the area, a detailed inspection of vehicles which fail or do not timely receive preclearance occurs. Vehicles which may not receive preclearance (not permitted to bypass the station) may include those providing a cargo bonding breakage signal, an indication of improper or errored credentials or manifest data and the like or presenting safety issues such as faulty brake or related signals. Whether or not monitored, driver

health issues may also be checked (for example, vision or drug/alcohol levels). The inspections may be random, i.e., ordered as a result of proper data reporting but nevertheless a no-go signal is signaled to the particular vehicle 200. If the vehicle safety, driver health or driver safety (overspeed or erratic activity) are signaled as problematical, each of these in turn may be checked or inspected.

Thus, as described above, an embodiment of the present invention may provide for a vehicular data processing method for use by a vehicle in crossing a border comprising the steps of initiating a request for preclearance or automatically receiving a polling signal; responsive to a polling signal, transmitting at least vehicle credential data; and receiving a bypass signal or a stop signal, the bypass signal indicating that the vehicle may pass and the stop signal indicating the vehicle must stop. Preferably the data is transmitted in a secure manner as will be further described in connection with Figure 4. Other related methods that will be further described herein include the automatic monitoring of safety equipment, driver credential, driver health or driver safety by police, the automatic monitoring of cargo bonding devices and cargo temperature, cargo weight, tariff payment and the like.

Now referring to Figure 3A, there is shown one alternative embodiment of an electronic vehicle log according to the present invention. A further embodiment is described by Figure 3B and yet a third embodiment is described by Figure 3C. From a study of each embodiment, one of skill in the art will be prepared to design an electronic vehicle log for a particular application and/or vehicle type and, in accordance with Figure 4, design an appropriate security method and means depending on the level of security desired.

Figure 3A shows an in-vehicle data processing interface unit. Box 300 exemplifies a housing for housing components of an EVL according to the present invention. The EVL system apparatus 300 includes, for example, a radio or other vehicle-to-roadside, vehicle-to-vehicle or vehicle-to-aircraft communications apparatus 301. Examples of short range devices that may be used include a Hughes Radio or Mark IV (MkIV) units or other similar radio systems known in the art or so-called automatic vehicle identification units. Longer range communication may be cellular radio via telephone modem or 220MHz radio manufactured by Scientific-Atlanta and other suppliers. Also, Qualcomm Omnitrax provides longer range communications.

Apparatus 301 is coupled between a suitable antenna (via link 309) and computer processing unit 302. Similarly situated is systems applications apparatus 303 for, for example, receiving GPS or Loran or other location and time update data via an antenna via link 310. Other functions of apparatus 303 include security and built-in-test (BIT) test circuitry. Processing set 302 and systems applications apparatus 303 may be powered by the vehicle battery via a 12-volt power inverter or other circuitry 304. Computer processing set 302 houses the processor, non-volatile (software algorithm) memory, PCMCIA (card or module) receiver, analog/digital interfaces as necessary, operator/machine interfaces as necessary and built-in test circuitry. The plug-in security EVL module is represented by both 307a and 308a for storing fixed and variable data respectively via respective links 307 and 308. Fixed data 307a of an EVL includes and should not be considered to be limited to include cab identification data, truck line identification data, registration data, location data and the like. Variable data 308a may be considered to include and not be limited to include driver identification data, trailer identification data, load identification data, route data, initial weight data, credentials and fees data, hazardous material data and safety inspection data.

Of course, one purpose of the device 300 and log 307a, 308a is to provide via antenna(s) 309 certain outputs 310a responsive to certain external inputs 309a. Inputs 309a comprise the polling request and the identification of the poller. Once the polling request is made, data returned and authorization determined a preclearance authorization signal is another input. Yet another input may be a request to stop for a detailed inspection as has been already described above that may be an alternative to a preclearance authorization signal. The outputs 310a, typically provided in response to a poll, comprise the identification, classification and location of the vehicle and driver. As necessary, a preclearance request signal may be generated. Other credentials necessary for polling site preclearance are provided as necessary. The safety/health of the vehicle/operator may be output. Also, there may be provided a mileage and fuel report for purposes of comparing with intended route and typical fuel consumption figures.

Processor 302 is linked to on-board sensors via link 305 which may be wired or wireless. Vehicle sensor data 305a comprises driver condition data (for example,

alcohol sensors for intoxication determination), load condition/security (temperature, bonding), vehicle condition (engine temperature)/security and the like and internal data processing unit security sensing (the BIT test) among others too numerous to list.

Processor 302 is also linked, for example, as necessary to alternatives to known short range roadside polling devices via known in the art systems described above such as automatic vehicle identification systems. These devices return data to the inspection facility responsive to inspection facility initiated polling requests by alternative means.

Thus, there is provided apparatus for maintaining an electronic log of vehicular activity for an automatic border crossing comprising radio apparatus for communicating with an inspection facility and for periodically receiving time and location data. Protected data packets as electronically signed and stored in variable data EVL 308a as will be described in connection with Figure 4.

Yet another preferred embodiment of an in-vehicle unit is shown in Figure 3B. While the whole of Figure 3B is labeled as an Electronic Vehicle Log, Figure 3B is similar to Figure 3A in that box 350 represents a housing in which are situated elements including a processor and memory and connections are shown to other elements outside the housing such as the EVL log media 370 preferably comprising a disk, flash memory, card or other NVM. For simplicity, Figure 3B does not show a microphone, all the optional sensors, the antennas for wireless communication and the like shown in Figures 1 or Figure 3A.

In particular, within box 300 are a bus system 356 for coupling various circuits together and providing intercommunication at a sixteen bit level such as an International Standards Authority (ISA) standard bus system known in the art. The ISA bus 356 provides 16 bit data lines and 24 bit address lines for addressing and retrieving data from memories connected thereto. Connected to the bus 356 are a processor 351, a PCMCIA controller 352, a flash memory 353, a volatile memory 354 and an interface controller such as a quad serial interface controller 355. Sample capacities, not intended to be limiting the present invention, are 512 kbytes for volatile memory 354 and flash memory 353.

Processor 351 provides the intelligence for the unit and may comprise, for example, an ELAN 80386 integrated processor or other microprocessor. The "386"

processor has internal random access memory and program memory which may be insufficient for the present purposes. Consequently, external flash memory 353 and volatile memory 354 are provided for providing sufficient capacity for the tasks at hand. Flash memory 353 is non-volatile and amy store fixed data such as the unit identification, algorithms and the like in permanent secure form. Volatile memory preferably random access memory provides working space for processor 351.

Controllers 352 and 355 provide slave control of input/output functions for the processor 351. PCMCIA controller 352 is coupled to the EVL credentials non-volatile memory 370 which may be in the form of one or more disks, flash memories, smart cards or other like removable secure memory which may be inserted into yet another processor (personal computer, mainframe, or like computer) for loading credential data prior to vehicle departure.

In particular, credentials may be inserted briefly into the PCMCIA slot, read into EVL volatile memory, and the credentials then removed freeing the slot. Alternatively, the credentials may be left in the EVL during the entire transit. In this case, the log may be placed on the same physical device as the credentials, or the spare PCMCIA slot 390 may be used as the EVL log memory device.

Controller 352 also handles input functions from a global positioning system card 380 known in the art. This card may be coupled to an antenna for periodically receiving real time of day and location data and storing the data in buffer memory for use by processor 351 for forming protected data packets as will be further described herein. The card may be clocked by a local oscillator and have an internal real time of day clock algorithm which is periodically maintained at a correct time of day by a satellite downlink signal received at an antenna (not shown).

Controller 352 also interfaces with a spare card that may be used for storing credentials, may comprise an analog interface or an interface to another bus system such as a vehicle bus system for collecting vehicle data (engine temperature, ignition, oil, fuel consumption, odometer and the like). The PCMCIA card 390 may have other applications which come to mind from a further study of the present invention.

Finally, controller 355 provides a plurality of, for example, RS232 serial line interfaces to, for example, digital cellular communications apparatus or Type 3 AVI tags for roadside-to-vehicle short range communications via link 395, to other

wireless communications via link 396, to additional sensors, such as digital sensors via link 397 different from those supported by card 390 and/or accessible through a vehicle bus and to a user interface via link 398 such as a keyboard, speech interface and/or display or speech synthesis interface.

These elements together perform the following functions. The processor 351 provides overall processing control and includes the internal capabilities to control two PCMCIA ports on its own, namely ports for PCMCIA cards 360 and 370. One (the EVL media or card 370) has already been described. The other is analog acquisition card 360 providing eight connections each for continuous and discrete analog signals, with the continuous signals typically digitized to 8 or 12 bits of resolution, for reception of such vehicle data as ignition switch position, speed, steering, brake accelerator data, tachometer data, electronic cargo bonding data and the like.

Some processors 351 desirably provide on-board One Time Programmable (OTP) memory which may be used to securely record the EVL-unique secret key and identification number. These are most desirably maintained as closed to the function of forming protected data packets as possible and desirably are not removed to FLASH memory 353 for fear of being intercepted and known by one not intended to possess them.

The FLASH memory 353 then is more desirably used for permanently storing the executable software. The memory 353 may be loaded at the time of manufacture with the EVL-unique secret key and identification number if that data is not included in the processor's (351) on-board OTP memory. All memory capacities, bus sizes, capabilities and speeds are nominal. For example, the unit may provide DRAM and FLASH memory sizes from 256 kilobytes to 1024 kilobytes or larger by utilizing alternate sized chips currently available. Currently available PCMCIA analog acquisition cards provide four to eight channels each of continuous or discrete inputs, but higher densities are anticipated and can be incorporated without changes to the unit's (300) hardware. Flexibility is enhanced using a PCMCIA design supporting cards for multiple functions and tasks. Alternatively the corresponding circuitry may be directly incorporated onto the unit's motherboard (similar to the design of Figure 3A) or placed onto a daughterboard interfacing the ISA bus 356. The latter design

may have a lower EVL hardware cost.

A third embodiment will be quickly described with reference to Figure 3C. In this embodiment, box 320 represents the data processing and information management function. Data processing power has been increased to the level of an integrated 486 type microprocessor 322 with approximately 256 kilobytes of flash memory 321 and 1 megabyte of DRAM 323. The processor interfaces with a data and information display and control function 335 including a keyboard or other input (not shown), touchscreen, or LCD, LCD controller and memory 336.

To receive input and provide output externally, there are provided parallel port 341 of the processor and serial port 342 of an external interface 340. Through the external interface 340, there pass cellular phone data, roadside reader or tag data, GPS data, satellite communications data (such as LEOSAT) and Qualcomm OmniTrax data.

There is also provided a PC-104 mezzanine interface.

To obtain vehicle and other sensor data, there is an eight channel analog sensor interface 330 designated 331 through which multi-sensor data is acquired. As has already been described, the sensors obtain safety, emission, cargo security and vehicle security and safety data among other data.

EVL data information storage and retrieval are represented by box 325 including a first and second PCMCIA interface 326 and 327 for electronic credential data of driver, cargo and vehicle.

Now referring to Figure 4, the operation of processors 302, 351 or equivalent processors will be described in connection with the formation of protected data packets (PDP's). Generally, Figure 4 represents the creation of the log memory of the Electronic Vehicle Log (EVL) 1 of the present invention. The protection provided for EVL memory 430 is described by outer dashed line box 433 as comprising a password and/or speaker verification. Via link 431 an EVL-unique secret key is provided to processor and DRAM 400 (for example, processor 302, 351).

Via link 401, the processor gathers the vehicle location data and via link 402 the processor gathers date and real time data, for example, from the same source 303 or 380 as described earlier in connection with Figures 3A and 3B.

Processor 400 also obtains vehicle sensor data via link 403, credentials and event data via link or links 404 and cargo status data via link 405.

The output of the processor 400 is a protected data packet forwarded via link 420 to a non-volatile log memory 410, for example, similar in form to variable data 308a or memory 370. An expanded view of the contents of a protected data packet 411 of the present invention is represented by block 411. The protected data packet 411 contains logged information 420a, a real time of day and date stamp 420b, a vehicle location stamp 420c, the unique vehicle identification 420d and an electronic signature 420e formed as will be described herein.

Logged information 420a may represent a printed page scanned from a page scanner or more data and thus may comprise megabytes of memory. On the other hand, a date and time stamp 420b may comprise just a hundred bytes of memory or less, for example, representing approximately twenty ASCII characters. Vehicle location data 420c including latitude and longitude may require ten to twenty bytes. Likewise, a vehicle identifier 420d may comprise just the equivalent of about twenty ASCII characters. On the other hand, the electronic signature 420e may require 200 bytes of data.

In general, the EVL log data will be generated using the following steps: 1) Data for logging will be acquired from various sources including, but not limited to, on-vehicle sensors, external systems and cargo monitors. The types of data logged and methods for acquiring the data have been described already above. 2) When a log entry is to be made, the EVL processor 400 will obtain the current date and time of day, vehicle location (at least in the form of latitude and longitude and possibly in the form of map location data such as route and mileage along a route from a given point), the EVL secret key and the EVL unique identification data. The processes for obtaining that data have likewise been described above. 3) The EVL processor prepares a protected data packet (PDP) using the information from step 2. The processor computes the packet's electronic signature 420e using a secure hash algorithm, a public key encryption algorithm and the EVL secret key. The PDP is then stored on the data logging medium (card, disk or the like).

Public key/private key encryption algorithms are known in the art including one formerly licensed through PKP Partners (a partnership of RSA and Cylink, which

has recently been ordered dissolved by an arbitrator in California). Another is promoted through the National Institute of Standards and Technologies in Gaithersburg, Maryland (N.I.S.T.). US Patents numbered 4,405,829, 4,424,414, 4,200,770, 4,218,582, 4,995,082 and 5,231,668 describe this technology.

Once the data has been logged into the EVL, various methods may be used to transmit or transport the PDP's to other systems which may require the information (owners, drivers or governmental authorities). Additional encryption techniques may be used during transmission to prevent information from becoming available to unauthorized third parties who may be tapping the communications channel.

Now, data logging, authenticated data distribution, secure data transmission and credential storage operations will be described with reference to Figures 4A and 4B. Figure 4B shows the public key encryption pairs used by different authorities. First, data logging will be described in the context of the driver entering log data by way of example. When the vehicle is to be used, the driver inserts the removable non-volatile log memory 430 for the duration of the trip. For example, a driver may obtain access and log into the EVL by inputing their speech, a password or a biometric 433 after inserting their card memory 430. Upon successful recognition of the password or biometric and/or verification of the speaker's identity or after completion of both processes, the driver-unique data is used to decrypt a secret or private key member (for example, 451a which is never released from secure memory) of a public key encryption pair 451a and 451b. When data is to be logged by the driver, protected data packets containing this log data are generated with digital signatures formed by encrypting digital hash values with this secret key member 451a of the public key pair.

Now, authenticated data distribution will be described. Protected data packets (PDP's) 420 are transmitted to a requesting user via electronic means, for example, wireless, telephone modem or a memory card. The requesting user has a trusted (escrowed) copy of the public key 451b of the above-referenced public key pair 451a, 451b, the pair including the secret key 451a (which never leaves secure memory) used for forming the electronic signature. The public key 451b is used to verify that the electronic signature of the PDP is accurate. Correct verification of the electronic signature then confirms the data source (the driver-protected secret key 451a) and the

integrity of the data (since the hash value matches the PDP data).

Secure data transmission from one party to another or intra-party will now be described. A governmental authority may obtain access by a defined process. One example of such a process for obtaining an early transmission of vehicle data in advance of a border crossing or like event is described by the following. The agency wishing to receive secure data generates a public key encryption pair 452a, 452b different from that used by the driver and distributes the public key portion 452b to any person or system desiring to transmit secure data. The public key portion 452b is stored in EVL memory. A profile of a commercial vehicle and a cargo may be extracted from the vehicle via a card memory or may be electronically extracted by wireless means prior to the vehicle's departure and delivered to the authority with the stored public key portion 452b. The EVL generates a private encryption key 431 and uses it to encrypt PDP's with their corresponding digital signatures. The EVL encrypts this private encryption key 431 using the public key 452b and transmits that information to the agency receiving the data. The receiving agency decrypts the EVL private encryption key 431 using the secret key portion 452a of the key pair 452a, 452b and then decrypts the PDP's using the decrypted key 431. The profile and public key 452b are transmitted via a centralized authority data base to regional data bases for distribution to checkpoints, port of entry border crossings and the like along the intended route of the vehicle.

As the vehicle approaches the inspection facility, the vehicle is polled or interrogated, for example, preferably by wireless means in advance of reaching the facility so the vehicle need not stop its movement. The vehicle transmitted profile data is compared with the previously transmitted profile data and the inspector may preclear the vehicle through the inspection station. If the inspection data is a weigh station, for example, and data is to be entered into the log by the authority, an electronic signature is utilized to verify the entered data, preventing subsequent modifications of the logged information. Moreover, at the time the entry is made, the vehicle position and time from the global positioning system may be automatically and simultaneously recorded, allowing detection of fraudulent entries. As the vehicle crosses the border, a short range communications system may be used to verify that the vehicle crossing the border is the vehicle which received the preclearance to

cross.

It is also possible that the vehicle may carry all the profile information in the EVL and transit the data via wireless means to the authority just a few minutes before arrival or before the approval (for example, preapproval at a border crossing) event. In this case and in that described above as well, some sort of short range transmission is useful as the vehicle crosses the border to physically confirm that the vehicle crossing the border is the same as the one that provided the profile and credentials data and received preapproval to cross.

Finally, credential data storage will be described in some detail. An authorized individual such as an inspector or police officer creates a digital credential in a generating device's memory, for example, a laptop personal computer. A secret key 454a of a public key pair 454a, 454b is used to generate a digital signature for the credential data. The credential and signature are transmitted to the EVL using various means, possibly including wireless means, direct input (typing), or memory card transfer. This transfer may be encrypted as discussed above as desired. for wireless or other secure data transmission. The credential and signature are formed into a PDP and logged as described above for the driver data logging operation. When the credential is subsequently transmitted to a requesting agency, the agency will use a trusted copy of the public key portion 454b to verify the electronic signature of the PDP.

The EVL will internally store the data for subsequent display, processing or transmission. Much of the data stored will be sensitive. For example, the tariff-related data may be used to facilitate international border crossing and if this data could be electronically forged, it would result in a loss of revenue or worse. The storage techniques described above respond to this need for data security. The storage approach is also related to the data reception and transmission approaches described above and further in the following discussion.

A wide variety of media and storage techniques are currently available, several have been described above. One form is a removable non-volatile memory. This may comprise flash memory or other non-volatile memory adapted to form a removable unit such as a PCMCIA card. One or more of these cards may comprise the EVL.

Another memory is a removable disk drive. This may comprise a floppy disk drive or removable hard disk drive such as one, likewise mounted on a PCMCIA card. This may likewise be secure enough to form an EVL.

An internal non-volatile memory or disk drive may likewise comprise an EVL. This storage device may be hosted entirely within the EVL housing 300, 350 of Figures 3A or 3B. In one embodiment, it may not be removed without destruction of the data contained within.

In yet another embodiment of the present invention, an internal volatile memory may be used as an EVL if protected from erasure, for example, by a battery pr other power back-up device permanently associated therewith.

On the other hand, removable memory will allow a certified person to place credentials or event data on the storage device by removing it from the EVL housing, placing it into another electronic device (such as a portable computer), and writing the credentials in a secure manner onto the memory device. Non-volatile memory would require an interface between the EVL housing and the certified persons' electronic device. This interface could be either wired or wireless (radio frequency).

Typically each discrete group of information to be protected is processed by assembling the data in an area of volatile memory. The date and time of the packet creation are obtained from a reliable source and added to the packet. GPS and a clock internal to the EVL are possible sources. The position of the vehicle at the time of the packet creation are obtained from a reliable source and added to the packet. GPS and Loran are possible sources. The EVL unique identification data is obtained and added to the packet. A secure hash value is computed for the packet from the above-acquired data. The secure hash value is then encrypted using the EVL unique secret key from a public key encryption key pair. The encrypted secure hash value, then, is the electronic signature for the packet which may be recovered by those having the key to the exclusion of others. Packets with their corresponding signatures are stored in the EVL on the various storage media chosen for the application as described above.

The addition of reliable date, time of day, and location data is a significant security feature. It can prevent an unscrupulous person skilled in the art of computer hardware and software manipulation from forging protected data packets and inserting

them into the EVL memory when the EVL is at a location inconsistent with the legitimate position or at a time inconsistent with an expected time of day for legitimate packet creation.

To prevent unscrupulous, technically adept persons from obtaining illicit access to the EVL Secret Key and creating forged PDP's, the EVL secret key and EVL unique identification data may be further protected using other cryptographic or other technologies. For example, the EVL secret key and identification data may be encrypted by a password known only by the user (such as the driver). The user (driver) would be required to enter their password prior to the start of transit or the entry of their data. The unencrypted data would be maintained only as long as the vehicle travels and adheres to an intended route or defined itinerary prestored with the password of the driver.

As a further security means, PDP generation may be contingent upon successful completion of a Speaker Verification function within the EVL. For example, the EVL may include a speaker verification (identity verification) and speech recognition (password recognition) subsystem or subsystems which verbally accepts the password used to decrypt the EVL secret key and EVL identification data. If the registered vehicle driver's voice is not confirmed (through speaker verification, for example), then the PDP encryption is not performed.

Figure 5A provides a table as an example of a memory table of protected data packets that may be maintained in an in-vehicle database (EVL) according to the method of Figure 4. One item may be the vehicle identification data which uniquely identify at least the vehicle. In particular, however, for a particular trip, the data ideally describes a unique driver, a unique cab and a unique trailer or trailers if pulling more than one trailer at a time or during a route. Vehicle classification data may describe the type of vehicle/trailer(s) and an oversize or overweight condition. For example, some states require no trailer(s) having a greater length than a predetermined length for safety reasons as automobiles allegedly are unable to pass such long trailers. Vehicle height limits are important for bridge and tunnel construction. Weight limits are imposed for highways because overweight vehicles are an important cause of the failure of roadways over time.

Another data item is cargo description. Their are various types including

"hazardous" cargos that require special handling and special routing. Quantity must be logged and maintained for certain tariffs are based on quantity rather than weight or size. Cargo security is important to the trucker as well as the owner of the cargo. The cargo security is protected by bonding, by assuring environmental factors and the like. The cargo destination may vary with the route. Cargo is deposited and new cargo is picked up requiring new credential data be entered.

Route data comprises the following: intended route and intended stops along the way, alternate routes, expected times of arrival and destinations along the route. This data may be stored in the form of maps and compared with GPS data by appropriate algorithms to determine deviations from intended routes.

Safety information can contain inspections, dates of inspections, records of the inspections, and measurements taken. For example, brakes, engine failure, tire safety and the like, signal indicators and the like may be regarded over time.

Other credential data includes licenses permits, inspections, reports, trip logs of other trips, and manifests. This data is not intended to be entirely inclusive.

Over time, data may be tabulated and summarized and output in the form of Figure 5B. For example, brake performance can demonstrate over time the mechanical status and history of the cab and trailer(s) brakes. Moreover, over time, the driver status and history may be recorded. For example, the driver can collect road mileage, time or duration of travel for the mileage logged and health record. More particularly, the driver's vision, alcohol or drug record and the like can be maintained with the driver's identification. Figure 5B also refers to environmental systems for detecting temperature, pressure and the like which are factors of the environment of the vehicle, driver and cargo. Inspection records and on-board monitors and sensor data is recorded in an environmental system table over time.

Figures 6A and 6B provide charts showing several applications of the present invention identified as to service, application, technology or product applicable for providing that application, what can be demonstrated and its use. Figure 6B is merely a continuation of Figure 6A.

The following services are performed by the present invention in combination with external systems as required: commercial fleet management so that a fleet operator may maintain data on their fleet of vehicles, emergency notification and

personal security, hazardous material and incident notification, commercial vehicle electronic clearance and administrative procedures for state and international border crossing, automated roadside safety inspections and on-board safety monitoring. The reader will please refer to the charts for application, technology or product available, demonstration and utilization information for each of these.

Thus there has been shown and described an electronic vehicle log and security method therefore by which different users may apply their own electronic signatures and secure their own data for later retrieval. Data packets are protected from unscrupulous individuals who would forge data by not only protecting the packets via public key/private key encryption but by voice security and real time of day and location data. Deviations from the present invention may be practiced for any more of the services of Figures 6A and 6B or other services that may come to mind from a reading of the present application. Any pending applications or patents mentioned above should be deemed to be incorporated by reference as to any material contained therein that is essential to a proper understanding of the present invention's manufacture or use. The present invention should only be deemed to be limited by the scope of the claims which follow.

WHAT IS CLAIMED IS:

1. Apparatus for maintaining a log of credential data secure from an uncertified user comprising

a processor for forming protected data packets comprising at least the credential data and an electronic signature representing a certified user and

a memory for storing the protected data packets.

2. Log maintenance apparatus according to claim 1 further comprising means for providing date and time of day data for inclusion in the protected data packets.

3. Log maintenance apparatus according to claim 2 further comprising an interface to said processor for receiving vehicle location data.

4. Log maintenance apparatus according to claim 1 further comprising an interface to sensors for sensing in-transit data.

5. Log maintenance apparatus according to claim 1 further comprising an interface to means for obtaining cargo monitoring data.

6. Log maintenance apparatus according to claim 1 further comprising an interface to means for obtaining event data.

7. Log maintenance apparatus according to claim 3 wherein said protected data packets comprise credential data, date and time data, vehicle location data vehicle identification data and the electronic signature.

8. Log maintenance apparatus according to claim 3 further comprising a microphone coupled to said processor, said processor receiving voice samples via the microphone for comparison with voice data stored in the memory.

9. A vehicular data processing method for use by a vehicle in interacting with an in-transit facility comprising the steps of:

communicating with the in-transit facility;

receiving a polling signal;

responsive to the polling signal, transmitting at least vehicle credential data; and

receiving a bypass signal or a stop signal, the bypass signal indicating that the vehicle may pass and the stop signal indicating the vehicle must stop.

10. The data processing method of claim 9 wherein

preliminary to the transmitting step, generating protected data packets comprising the credential data and an electronic signature.

11. The data processing method of claim 10 wherein

preliminary to the transmitting step, collecting data representing the date and time of day for inclusion in the protected data packet.

12. The data processing method of claim 9 wherein

preliminary to the transmitting step, collecting data representing the location of the vehicle for inclusion in the protected data packet.

13. The data processing method of claim 9 wherein

preliminary to the transmitting step, collecting data representing a unique vehicle identification for inclusion in the protected data packet.

14. The data processing method of claim 9 wherein the electronic signature comprises a secure hash value computed for the packet encrypted using a secret key from a public key encryption key pair.

15. A method of generating protected data packets for storage in an electronic vehicle log comprising the steps of

collecting data to be protected,

collecting data representing date and time of day,

collecting vehicle location data,

retrieving vehicle identification data,

generating an electronic signature from one or more of the collected and retrieved data, and

storing the protected data packet including the data to be protected, the date and time of day, the vehicle location, the vehicle identification and the electronic signature.

16. The method of claim 15 wherein said electronic signature is generated by performing the steps of computing a secure hash value for the packet and encrypting the secure hash value using the secret key of a public key encryption key pair.

17. The method of claim 15 further comprising the steps of a user speaking a password for comparison with a password stored for the user.

18. The method of claim 15 further comprising the steps of

storing a private encryption key,

encrypting protected data packets for transmission using the private encryption key and

transmitting the protected packet using a public key pair different from one used in generating the electronic signature.

19. The method of claim 15 comprising the steps of

generating event data and

generating a further electronic signature for the event data using a public key pair different from one used in generating the electronic signature.

20. The method of claim 15 comprising the steps of

storing intended vehicle route data,

comparing the collected vehicle location data with the intended vehicle route data and

determining if the protected data packet is valid from the result of the comparison step.

FIG. 1

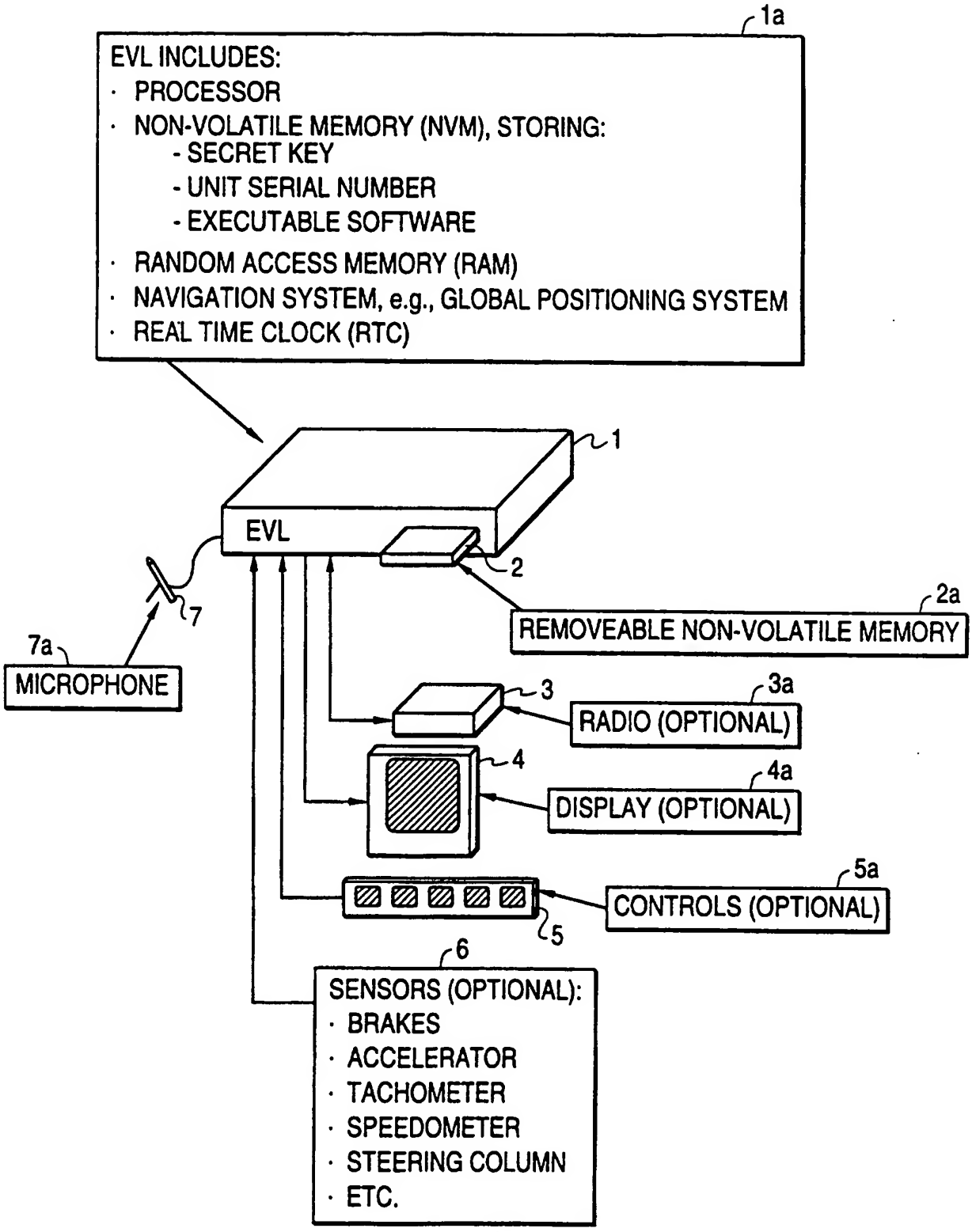

1a
EVL INCLUDES:
· PROCESSOR
· NON-VOLATILE MEMORY (NVM), STORING:
- SECRET KEY
- UNIT SERIAL NUMBER
- EXECUTABLE SOFTWARE
· RANDOM ACCESS MEMORY (RAM)
· NAVIGATION SYSTEM, e.g., GLOBAL POSITIONING SYSTEM
· REAL TIME CLOCK (RTC)
1
EVL
2
2a
REMOVEABLE NON-VOLATILE MEMORY
7
7a
MICROPHONE
3
3a
RADIO (OPTIONAL)
4
4a
DISPLAY (OPTIONAL)
5a
CONTROLS (OPTIONAL)
5
6
SENSORS (OPTIONAL):
· BRAKES
· ACCELERATOR
· TACHOMETER
· SPEEDOMETER
· STEERING COLUMN
· ETC.

FIG. 2A

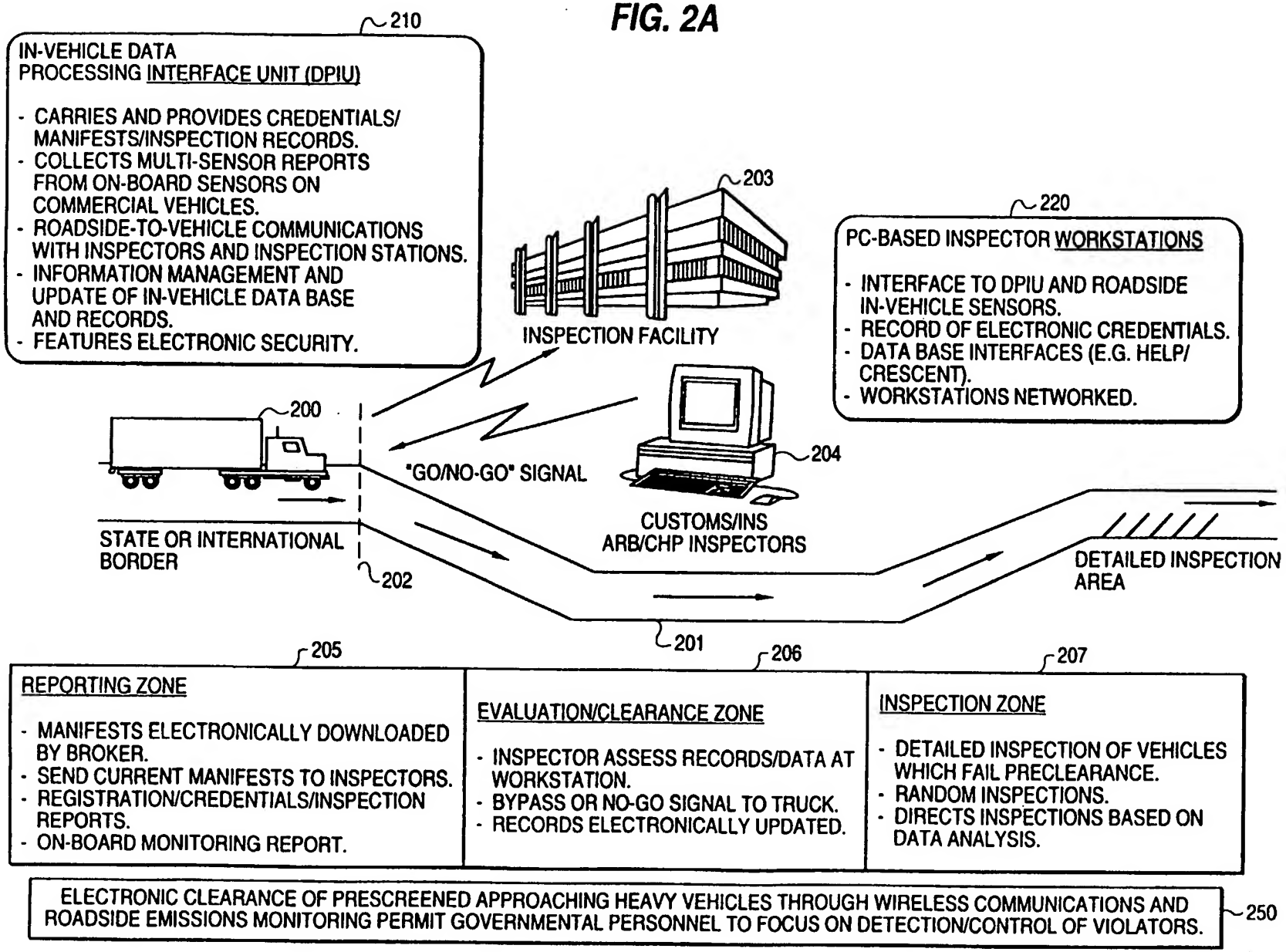

210
IN-VEHICLE DATA PROCESSING INTERFACE UNIT (DPIU)
- CARRIES AND PROVIDES CREDENTIALS/ MANIFESTS/INSPECTION RECORDS.
- COLLECTS MULTI-SENSOR REPORTS FROM ON-BOARD SENSORS ON COMMERCIAL VEHICLES.
- ROADSIDE-TO-VEHICLE COMMUNICATIONS WITH INSPECTORS AND INSPECTION STATIONS.
- INFORMATION MANAGEMENT AND UPDATE OF IN-VEHICLE DATA BASE AND RECORDS.
- FEATURES ELECTRONIC SECURITY.
203
INSPECTION FACILITY
220
PC-BASED INSPECTOR WORKSTATIONS
- INTERFACE TO DPIU AND ROADSIDE IN-VEHICLE SENSORS.
- RECORD OF ELECTRONIC CREDENTIALS.
- DATA BASE INTERFACES (E.G. HELP/ CRESCENT).
- WORKSTATIONS NETWORKED.
200
"GO/NO-GO" SIGNAL
204
CUSTOMS/INS ARB/CHP INSPECTORS
STATE OR INTERNATIONAL BORDER
202
DETAILED INSPECTION AREA
201
205
REPORTING ZONE
- MANIFESTS ELECTRONICALLY DOWNLOADED BY BROKER.
- SEND CURRENT MANIFESTS TO INSPECTORS.
- REGISTRATION/CREDENTIALS/INSPECTION REPORTS.
- ON-BOARD MONITORING REPORT.
206
EVALUATION/CLEARANCE ZONE
- INSPECTOR ASSESS RECORDS/DATA AT WORKSTATION.
- BYPASS OR NO-GO SIGNAL TO TRUCK.
- RECORDS ELECTRONICALLY UPDATED.
207
INSPECTION ZONE
- DETAILED INSPECTION OF VEHICLES WHICH FAIL PRECLEARANCE.
- RANDOM INSPECTIONS.
- DIRECTS INSPECTIONS BASED ON DATA ANALYSIS.
ELECTRONIC CLEARANCE OF PRESCREENED APPROACHING HEAVY VEHICLES THROUGH WIRELESS COMMUNICATIONS AND ROADSIDE EMISSIONS MONITORING PERMIT GOVERNMENTAL PERSONNEL TO FOCUS ON DETECTION/CONTROL OF VIOLATORS.
250

FIG. 2B

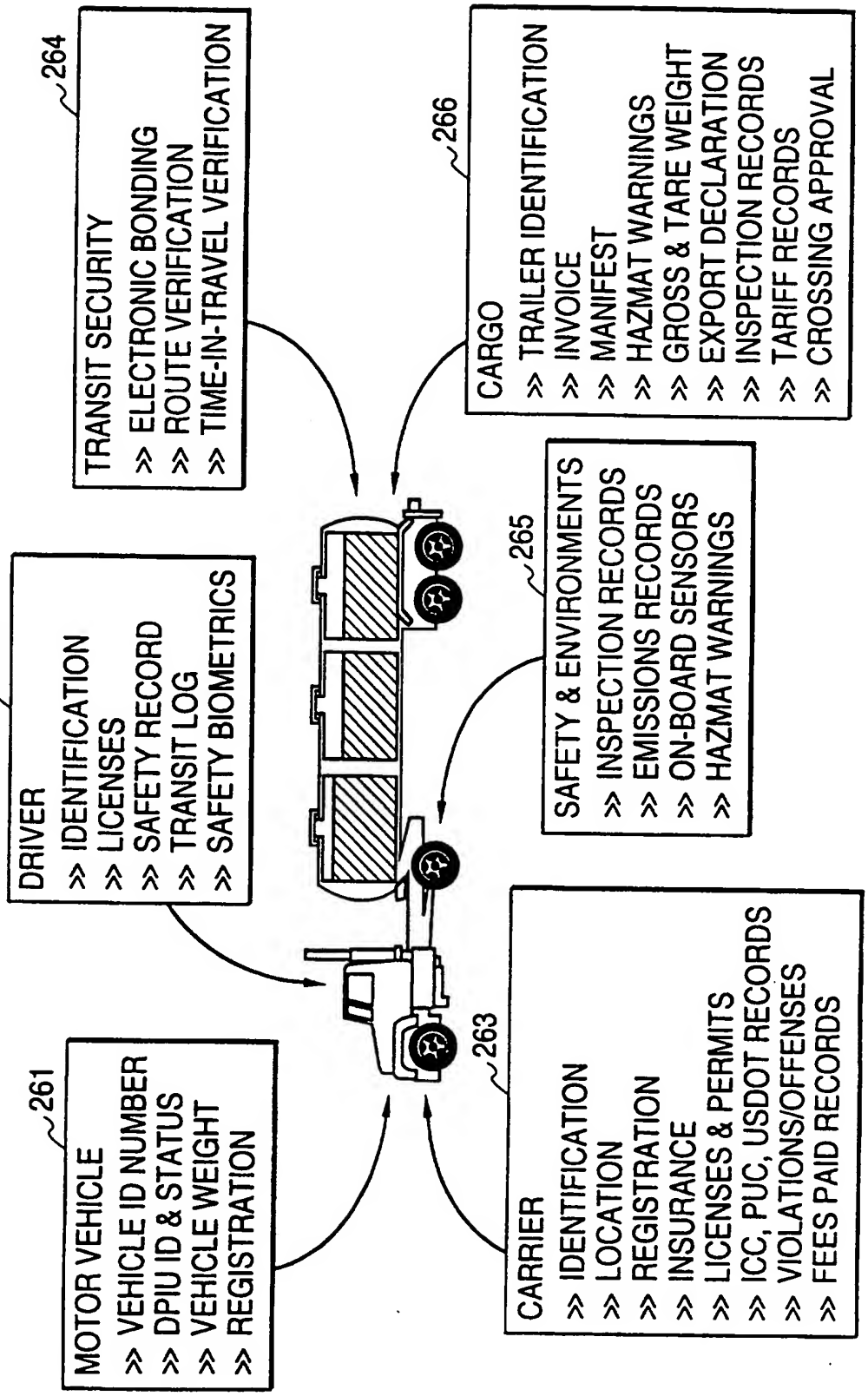

264
TRANSIT SECURITY
» ELECTRONIC BONDING
» ROUTE VERIFICATION
» TIME-IN-TRAVEL VERIFICATION
266
CARGO
» TRAILER IDENTIFICATION
» INVOICE
» MANIFEST
» HAZMAT WARNINGS
» GROSS & TARE WEIGHT
» EXPORT DECLARATION
» INSPECTION RECORDS
» TARIFF RECORDS
» CROSSING APPROVAL
262
DRIVER
» IDENTIFICATION
» LICENSES
» SAFETY RECORD
» TRANSIT LOG
» SAFETY BIOMETRICS
265
SAFETY & ENVIRONMENTS
» INSPECTION RECORDS
» EMISSIONS RECORDS
» ON-BOARD SENSORS
» HAZMAT WARNINGS
261
MOTOR VEHICLE
» VEHICLE ID NUMBER
» DPIU ID & STATUS
» VEHICLE WEIGHT
» REGISTRATION
263
CARRIER
» IDENTIFICATION
» LOCATION
» REGISTRATION
» INSURANCE
» LICENSES & PERMITS
» ICC, PUC, USDOT RECORDS
» VIOLATIONS/OFFENSES
» FEES PAID RECORDS

FIG. 3A

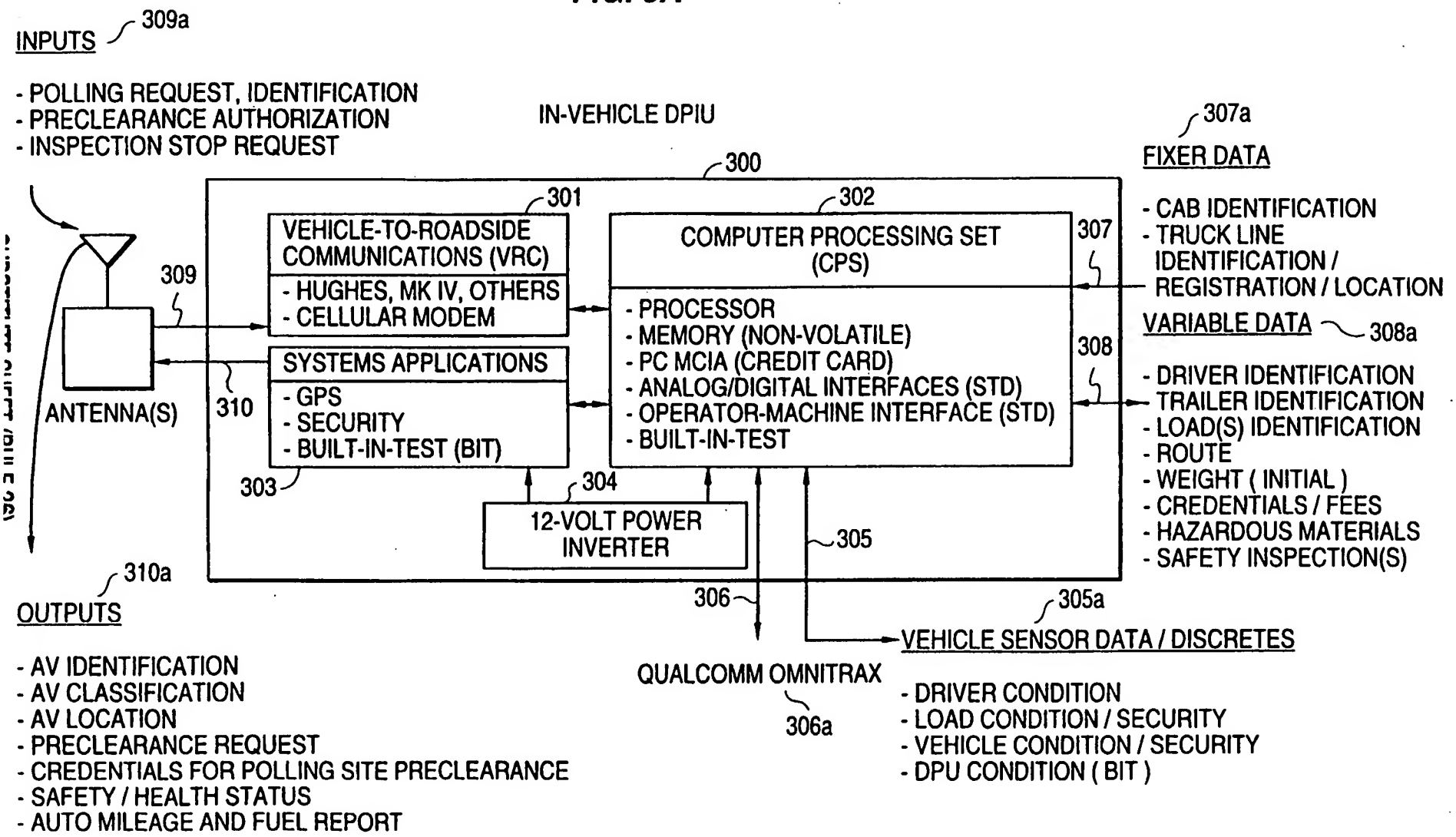

INPUTS
309a
- POLLING REQUEST, IDENTIFICATION
- PRECLEARANCE AUTHORIZATION
- INSPECTION STOP REQUEST
IN-VEHICLE DPIU
300
307a
FIXER DATA
- CAB IDENTIFICATION
- TRUCK LINE IDENTIFICATION / REGISTRATION / LOCATION
301
VEHICLE-TO-ROADSIDE COMMUNICATIONS (VRC)
- HUGHES, MK IV, OTHERS
- CELLULAR MODEM
302
COMPUTER PROCESSING SET (CPS)
- PROCESSOR
- MEMORY (NON-VOLATILE)
- PC MCIA (CREDIT CARD)
- ANALOG/DIGITAL INTERFACES (STD)
- OPERATOR-MACHINE INTERFACE (STD)
- BUILT-IN-TEST
307
308
VARIABLE DATA
308a
- DRIVER IDENTIFICATION
- TRAILER IDENTIFICATION
- LOAD(S) IDENTIFICATION
- ROUTE
- WEIGHT (INITIAL)
- CREDENTIALS / FEES
- HAZARDOUS MATERIALS
- SAFETY INSPECTION(S)
309
ANTENNA(S)
310
SYSTEMS APPLICATIONS
- GPS
- SECURITY
- BUILT-IN-TEST (BIT)
303
304
12-VOLT POWER INVERTER
305
310a
OUTPUTS
- AV IDENTIFICATION
- AV CLASSIFICATION
- AV LOCATION
- PRECLEARANCE REQUEST
- CREDENTIALS FOR POLLING SITE PRECLEARANCE
- SAFETY / HEALTH STATUS
- AUTO MILEAGE AND FUEL REPORT
306
QUALCOMM OMNITRAX
306a
305a
VEHICLE SENSOR DATA / DISCRETES
- DRIVER CONDITION
- LOAD CONDITION / SECURITY
- VEHICLE CONDITION / SECURITY
- DPU CONDITION (BIT)

FIG. 3B

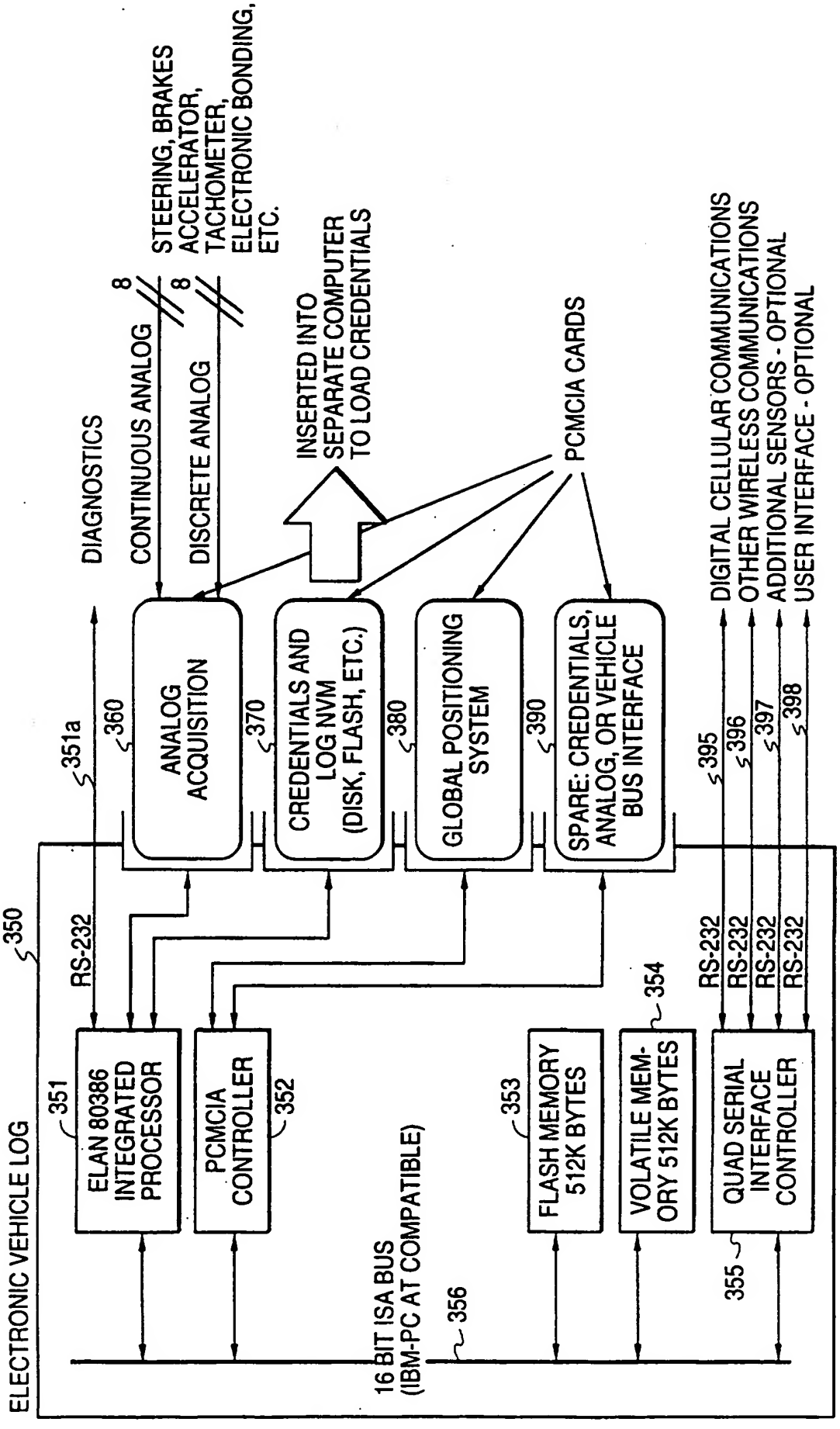

ELECTRONIC VEHICLE LOG
350
351
ELAN 80386 INTEGRATED PROCESSOR
352
PCMCIA CONTROLLER
353
FLASH MEMORY 512K BYTES
354
VOLATILE MEMORY 512K BYTES
355
QUAD SERIAL INTERFACE CONTROLLER
356
16 BIT ISA BUS (IBM-PC AT COMPATIBLE)
RS-232
351a
DIAGNOSTICS
360
ANALOG ACQUISITION
370
CREDENTIALS AND LOG NVM (DISK, FLASH, ETC.)
380
GLOBAL POSITIONING SYSTEM
390
SPARE: CREDENTIALS, ANALOG, OR VEHICLE BUS INTERFACE
8
CONTINUOUS ANALOG
8
DISCRETE ANALOG
STEERING, BRAKES ACCELERATOR, TACHOMETER, ELECTRONIC BONDING, ETC.
INSERTED INTO SEPARATE COMPUTER TO LOAD CREDENTIALS
PCMCIA CARDS
395
396
397
398
DIGITAL CELLULAR COMMUNICATIONS
OTHER WIRELESS COMMUNICATIONS
ADDITIONAL SENSORS - OPTIONAL
USER INTERFACE - OPTIONAL

FIG. 3C

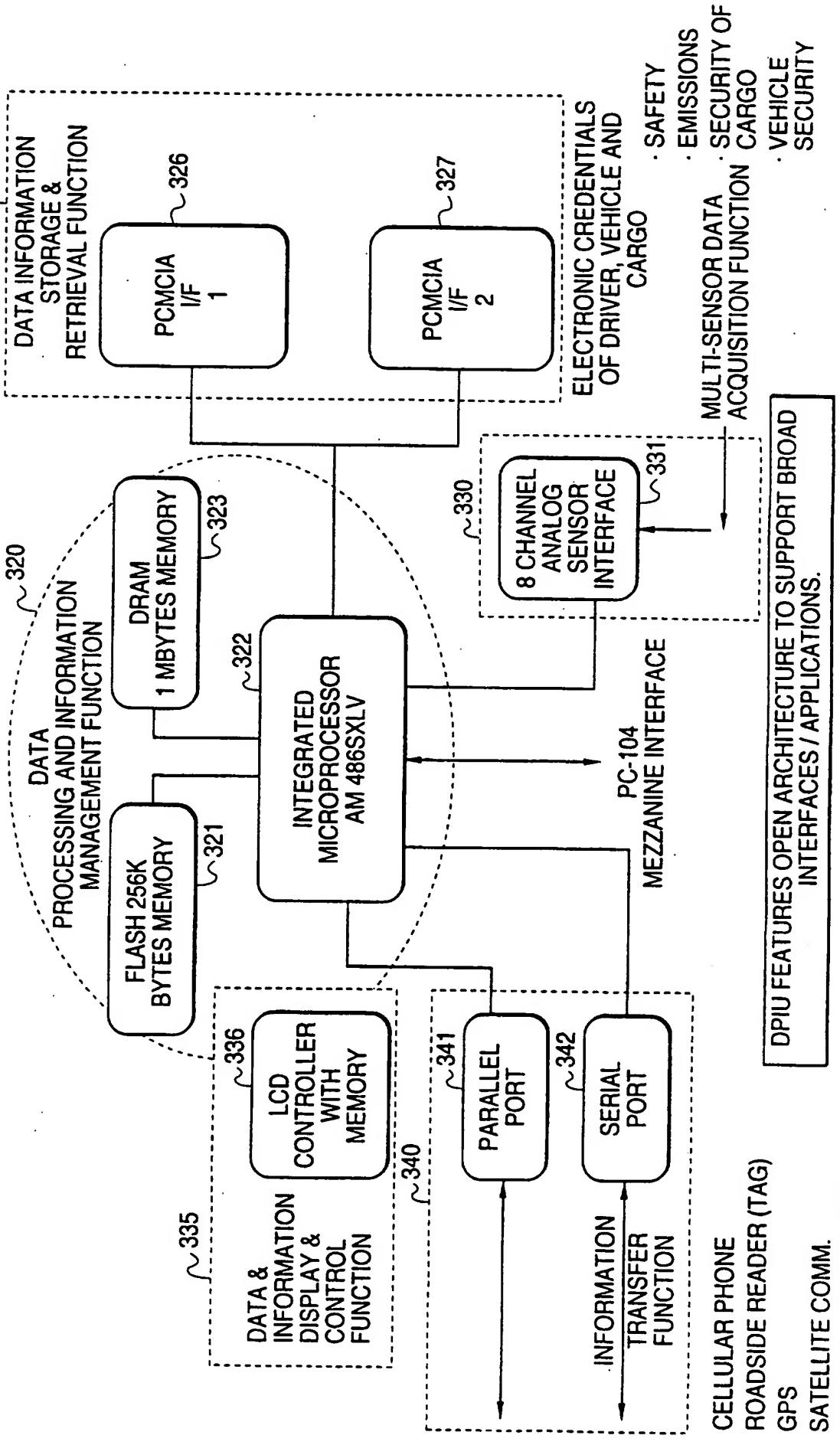

325
DATA INFORMATION STORAGE & RETRIEVAL FUNCTION
326
PCMCIA I/F 1
327
PCMCIA I/F 2
ELECTRONIC CREDENTIALS OF DRIVER, VEHICLE AND CARGO
· SAFETY
· EMISSIONS
· SECURITY OF CARGO
· VEHICLE SECURITY
MULTI-SENSOR DATA ACQUISITION FUNCTION
330
8 CHANNEL ANALOG SENSOR INTERFACE
331
320
DATA PROCESSING AND INFORMATION MANAGEMENT FUNCTION
323
DRAM 1 MBYTES MEMORY
322
INTEGRATED MICROPROCESSOR AM 486SXLV
321
FLASH 256K BYTES MEMORY
PC-104 MEZZANINE INTERFACE
DPIU FEATURES OPEN ARCHITECTURE TO SUPPORT BROAD INTERFACES / APPLICATIONS.
335
DATA & INFORMATION DISPLAY & CONTROL FUNCTION
336
LCD CONTROLLER WITH MEMORY
340
INFORMATION TRANSFER FUNCTION
341
PARALLEL PORT
342
SERIAL PORT
CELLULAR PHONE
ROADSIDE READER (TAG)
GPS
SATELLITE COMM.
QUALCOMM OMNI TRAX

FIG. 4A

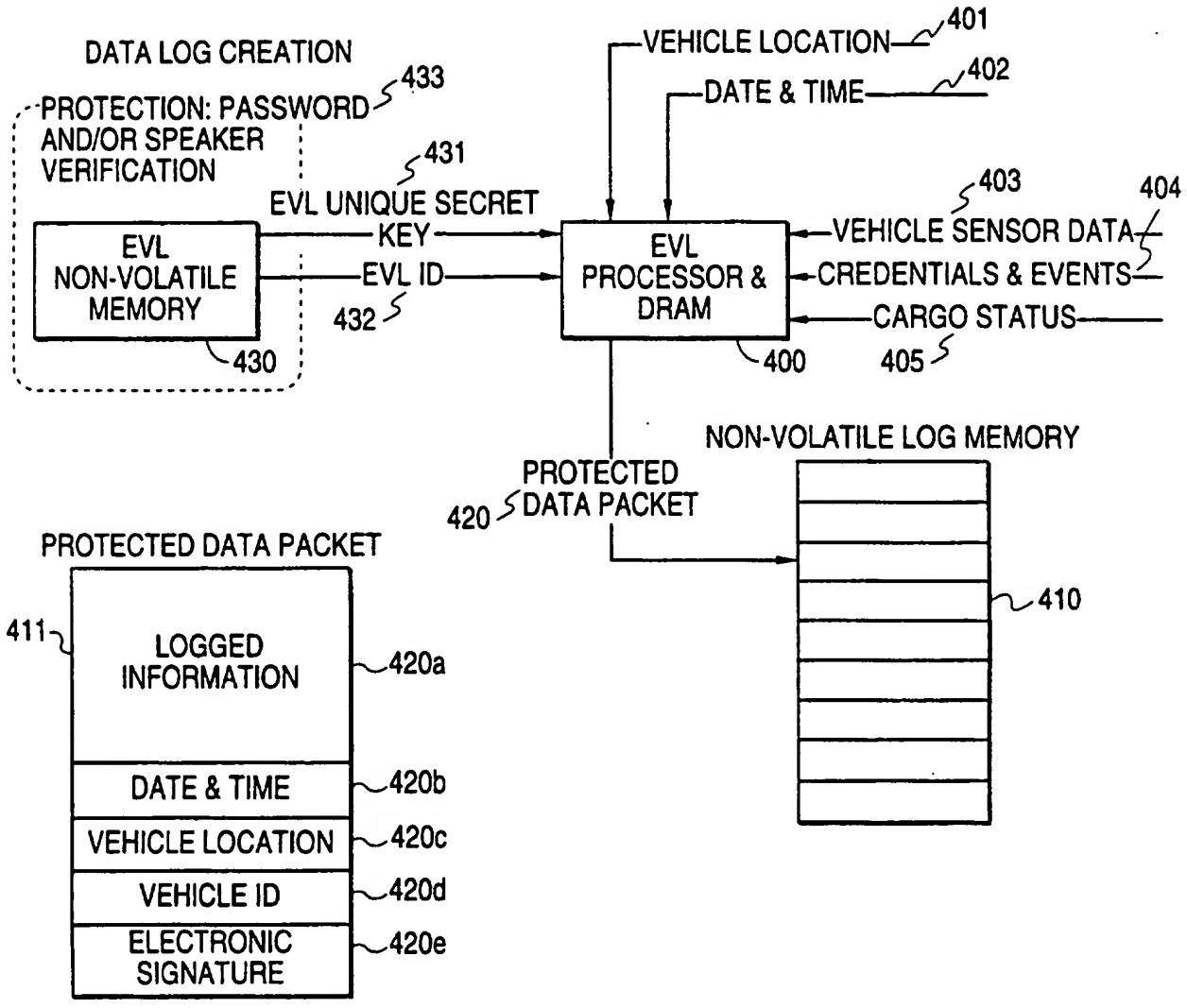


FIG. 4B

		DRIVER	3RD PARTY AUTHORITY	OWNER-TRUSTED AUTHORITY
PUBLIC KEY PAIR	PRIVATE KEY	451a	452a	454a
	PUBLIC KEY	451b	452b	454b
EVL KEY			431	

FIG. 5A

ITEM	CONTENTS
VEHICLE IDENTIFICATION	DRIVER, CAB, TRAILER(S)
VEHICLE CLASSIFICATION	TYPE OF VEHICLE/TRAILER(S) OVERSIZE/OVERWEIGHT
CARGO	TYPE / QUANTITY / SECURITY DESTINATION
ROUTE	ROUTES / STOPS/ DESTINATIONS / TIMES
SAFETY INFORMATION	INSPECTION DATES / RECORDS / MEASUREMENTS
CREDENTIALS	LICENSES / PERMITS / INSPECTIONS / REPORTS/ TRIP LOGS / MANIFESTS

FIG. 5B

ELEMENT	CHARACTERISTICS
BRAKE PERFORMANCE	MECHANICAL STATUS
DRIVER STATUS / HISTORY	ROAD MILES/ TIME / HEALTH RECORD
MAINTENANCE RECORDS	HISTORY / VIOLATIONS
ENVIRONMENTAL SYSTEM	INSPECTION RECORDS / ON-BOARD MONITORS

FIG. 6A

SERVICE	APPLICATION	TECHNOLOGY OR PRODUCT APPLICABLE	DEMONSTRATION	UTILIZATION
COMMERCIAL FLEET MANAGEMENT	- COMMERCIAL VEHICLE PRECLEARANCE SERVICE AT REAL TIME COMMUNICATIONS OF INFORMATION BETWEEN COMMERCIAL VEHICLE DRIVERS, DISPATCHERS AND INTERMODAL TRANSPORTATION PROVIDERS. - REAL TIME ROUTE PLANNING AND RE-PLANNING. - JUST-IN-TIME DELIVERY AND PICK-UP CAPABILITY. - REAL TIME TRAFFIC INFORMATION. - ELECTRONIC PURCHASING CREDENTIALS FOR SHIPMENTS. - AUTO MILEAGE AND FUEL REPORTING AND AUDITING	- COMMUNICATIONS INFRA-STRUCTURE. - AUTOMATIC VEHICLE/DRIVER MONITOR/ID SYSTEM. - ADVANCED INFORMATION MANAGEMENT - ROUTE PLANNING AND RE-PLANNING - ADVANCED TRAFFIC INFORMATION/MANAGEMENT SYSTEM. - MILEAGE AND FUEL USAGE MONITORING AND RECORDING.	- IN-VEHICLE-TO-ROAD-SIDE (DISPATCHER) COMMUNICATIONS NETWORK SERVICE. - ON-BOARD SENSORS AND PROCESSORS. - TWO-WAY DIGITAL AND VOICE COMMUNICATIONS SYSTEM. - COMMUNICATIONS/DATA SECURITY.	- PRIVATE SECTOR: - TRUCK LINES AND TRANSPORTATION PROVIDERS (RR).
EMERGENCY NOTIFICATION AND PERSONAL SECURITY	- IMMEDIATE NOTIFICATION OF AN INCIDENT AND IMMEDIATE REQUEST FOR ASSISTANCE. -DRIVER SECURITY (MANUALLY INITIATED NOTIFICATION AND REQUEST FOR SUPPORT). - MECHANICAL BREAKDOWNS. - TRUCK JACKING. - NON-INJURY ACCIDENTS. - AUTOMATED COLLISION NOTIFICATION/ REQUEST FOR ASSISTANCE. - TRAFFIC CONGESTION INCIDENT/ POTENTIAL NOTIFICATION AND REQUEST FOR SUPPORT.	- VEHICLE/DRIVER POSITION AND ID. - CARGO ID. - ID OF INCIDENT AND TYPE OF SUPPORT REQUIRED. - EMERGENCY SERVICES COMMUNICATIONS. - NETWORK-IN-VEHICLE-TO-ROADSIDE COMMUNICATIONS. - ADVANCED INFORMATION MANAGEMENT SYSTEM.	N/A	-CARRIERS/TRUCK LINES. - EMERGENCY SERVICE. - MECHANICAL REPAIR SERVICES. -AUTOMATED TRAFFIC INFORMATION MANAGEMENT CENTERS.
HAZARDOUS MATERIAL AND INCIDENT NOTIFICATION	- MONITORING INTERMODAL TRANSPORTA-TION OF HAZMAT. - NOTIFICATION OF HAZMAT SHIPMENT THROUGH CITY, STATE, COUNTRY. - NOTIFICATION OF INCIDENT INVOLVING HAZMAT SHIPMENT.	- DIRECTION OF RESPONSE TEAMS TO INCIDENT. - NOTIFICATION OF ENFORCE-MENT AGENCIES OF SHIP-MENTS. - ID, CLASS AND LOCATION OF SHIPMENT. - PRECLEARANCE CREDENTIALS.	N/A	- HAZMAT SHIPMENT VEHICLES. - GOVERNMENT AGENCIES. - RESPONSIBLE FLEET MANAGEMENT.

FIG. 6B

SERVICE	APPLICATION	TECHNOLOGY OR PRODUCT APPLICABLE	DEMONSTRATION	UTILIZATION
COMMERCIAL VEHICLE ELECTRONIC CLEARANCE AND ADMINISTRATIVE PROCESSES	- DOMESTIC PRECLEARANCE. - WEIGHT - CREDENTIAL - SAFETY/HEALTH - CARGO - BORDER PRECLEARANCE.	- VEHICLE TO/FROM ROADSIDE COMMUNICATIONS. - INFORMATION EXCHANGE SYSTEM SECURE. - HIGH-SPEED WEIGHT-IN-MOTION SYSTEMS. - VEHICLE POSITION MONITORING AND ID - AVC. - DRIVER AND DRIVER RECORDS MONITORING.	- IN-VEHICLE PROCESSOR/DATA BASE/COMMUNICATIONS INTERFACE. - COMMUNICATIONS NETWORK: VEHICLE-TO ROADSIDE PROCESSOR AND ROAD-SIDE PROCESSOR-TO-CENTRAL CONTROL.	- STATES. - CARRIERS (TRUCKS AND RAIL) - COUNTRIES: - CANADA. - MEXICO. - USA.
AUTOMATED ROADSIDE SAFETY INSPECTION	- SUPPORT PRECLEARANCE CAPABILITY. - SAFETY OF HIGHWAYS. - BREAKS. - DRIVER CONDITIONS. - VEHICLE SYSTEMS. - SAFETY PERFORMANCE RECORD OF CARRIER, VEHICLE, DRIVER INSPECTION AND VERIFICATION. - CORRECTIVE ACTIONS ORDERED AND TAKEN REVIEW.	- DRIVER/VEHICLE HISTORY FILES REAL TIME UPDATE. - COMMUNICATIONS VEHICLE TO CENTRAL VEHICLE DATA BASE. - VEHICLE MONITORING SYSTEM ON-BOARD DIAGNOSTIC. - VEHICLE/DRIVER ID AND CREDENTIALS REVIEW.	- IN-VEHICLE PROCESSOR WITH CREDIT CARD MEMORY FOR SAFETY/HEALTH HISTORY. - COMMUNICATIONS NETWORK AND INTERFACE FOR REAL TIME UPDATE OF RECORDS.	- ROADSIDE INSPECTIONS - STATE/FEDERAL. - TRUCK LINES. - PRECLEARANCE.
ON-BOARD SAFETY MONITORING	- COMMERCIAL VEHICLE PRECLEARANCE SERVICE AT CHECKPOINTS AND BORDER. - SUPPORT AUTOMATED ROADSIDE SAFETY INSPECTION SERVICE. - REAL TIME MONITORING CRITICAL COMPONENTS OF VEHICLE, CARGO, AND DRIVER.	- ON-BOARD SENSING/MONITORING THE SAFETY STATUS OF THE VEHICLE, CARGO AND DRIVER. - COMMUNICATIONS OF SAFETY/HEALTH STATUS TO OFF-BOARD NODE-VEHICLE-TO-ROADSIDE. - VEHICLE ID, DRIVER ID. - ON-BOARD PROCESSOR. - MONITORING/SENSING AND COLLECTING THE CONDITION OF CRITICAL VEHICLE COMPONENTS; BRAKES, TIRES, LIGHTS, SUSPENSION, STEERING, ETC. - SHIFT IN CARGO OR CARGO STATUS SENSING. - DRIVER HEALTH AND SAFETY MONITORING/REPORTING.	- IN-VEHICLE PROCESSOR/DATA BASE/COMMUNICATIONS INTERFACE. - SAFETY/HEALTH MONITORING SYSTEM ON-BOARD-DIAGNOSTIC AND WARNING SYSTEM. - COMMUNICATIONS NETWORK VEHICLE-TO-ROADSIDE NODE. - INTERROGATION OF VEHICLE PROCESSOR.	- CARRIERS. - NATIONAL ROADWAY SAFETY. - VEHICLE SAFETY INSPECTION AT MAINLINE SPEEDS.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/12459

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/40
US CL :364/424.02, 424.04, 550; 340/988, 426, 464, 825.31,825.34
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/424.02, 424.03, 424.04, 441, 550, 551.01; 340/988, 425.5, 426, 438, 464, 825.31,825.34

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y --- A	US, A, 4,754,255 (SANDERS ET AL) 28 June 1988, Figures 1, 3, and 5; column 2; column 3, lines 1-24; column 6, lines 46--68; column 7, lines 1+.	1-2 ------ 3-8,16,18 ----- 9-14,15,17,19-20
X --- Y --- A	US, A, 5,416,706 (HAGENBUCH) 16 May 1995, Figures 12-13, 14a-f.	15,20 ---- 3-5,7,16-19 ---- 9-14
Y --- A	US, A, 5,185,700 (BEZOS ET AL) 09 February 1993, Abstract; Figures 1-3 and 9-10	6,19 ---- 9-14

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 27 NOVEMBER 1995	Date of mailing of the international search report 01 FEB 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer COLLIN W. PARK Telephone No. (703) 305-9754

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/12459

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,856,072 (SCHNEIDER ET AL) 08 August 1989, Abstract; Figurs 1, 2, and 3c	8,17
A	US, A, 3,624,608 (ALTMAN ET AL) 30 November 1971, entire document.	1-20
A	US, A, 3,665,397 (DI NAPOLI ET AL) 23 May 1972, entire document.	1-20
A	US, A, 4,804,937 (BARBIAUX ET AL) 14 February 1989, entire document.	1-20
A	US, A, 4,910,493 (CHAMBERS ET AL) 20 March 1990, entire document.	1-20
A	US, A, 4,949,263 (JURCA) 14 August 1990, entire document.	1-20
A	US, A, 5,249,127 (KOMATSU) 28 September 1993, entire document.	1-20
A	US, A, 5,303,163 (EBAUGH ET AL) 12 April 1994, entire document.	1-8,15-20
A	US, A, 5,307,349 (SHLOSS ET AL) 26 April 1994, entire document.	9-14
A	US, A, 5,347,274 (HASSET) 13 September 1994, entire document.	1-20
A	US, A, 5,359,522 (RYAN) 25 October 1994, entire document.	1-8,15-20
A	US, A, 5,359,528 (HAENDEL ET AL) 25 October 1994, entire document.	1-20
A	US, A, 5,379,219 (ISHIBASHI) 03 January 1995, entire document.	1-8,15-20
A	US, A, 5,425,032 (SHLOSS ET AL) 13 June, 1995, entire document.	9-14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/12459

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/12459

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-8 and 15-20, drawn to a system of generating and maintaining a log.
Group II, claims 9-14, drawn to a method for use by a vehicle for interacting with an in-transit facility.

The inventions listed as Groups I and II do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:
Group I lacks the technical features of Group II representing its inventive concept, "communicating with the in-transit facility," "receiving a polling signal" from an in-transit facility, "transmitting vehicle credential data" to the facility, and "receiving a bypass or a stop signal." Further, Group II lacks the technical features of Group I, forming and storing "protected data packets."